(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－286904

(43)公開日　平成８年(1996)11月１日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	9/06	５５０		Ｇ０６Ｆ	9/06	５５０Ａ
	12/14	３２０			12/14	３２０Ｂ
Ｇ０９Ｃ	1/00	６１０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６１０Ｚ
		６６０	7259－5Ｊ			６６０Ｄ

審査請求　未請求　請求項の数９　ＯＬ　（全 11 頁）

(21)出願番号　特願平8－25674

(22)出願日　平成８年(1996)２月13日

(31)優先権主張番号　特願平7－25707

(32)優先日　平７(1995)２月14日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　秋山　良太
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　吉岡　誠
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

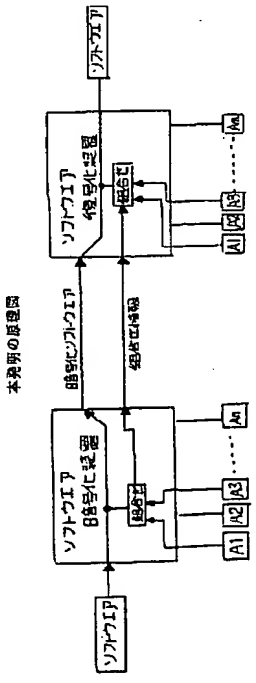
(74)代理人　弁理士　遠山　勉　（外１名）

(54)【発明の名称】　ソフトウエア暗号化・復号化方法、ソフトウエア暗号化システムおよびソフトウエア復号化システム

(57)【要約】

【課題】　暗号化ソフトウエアの不正解読を簡易な技術で防止する

【解決手段】　ソフトウエアを暗号化する際に、２以上の暗号化基本アルゴリズムを採用するようにした。一方、ソフトウエア復号化処理ではこの２以上の暗号化基本アルゴリズムに対応した復号アルゴリズムを用意した。そして、ソフトウエア暗号化処理では暗号化ソフトウエアとともに暗号化した基本アルゴリズムの組合せ情報をソフトウエア復号処理に引き渡す。ソフトウエア復号処理では、前記基本アルゴリズムの組合せ情報に基づいて自身の保有する逆アルゴリズムを選択して前記暗号化ソフトウエアを復号化するようにした。



1

【特許請求の範囲】

【請求項１】　２以上の暗号化基本アルゴリズムを組み合わせてソフトウエアを暗号化するソフトウエア暗号化ステップと、

暗号化されたソフトウエアを入力して前記暗号化に用いられた前記２以上の暗号化基本アルゴリズムの復号化アルゴリズムによって前記ソフトウエアを復号化するソフトウエア復号化ステップとからなり、

前記ソフトウエア暗号化処理は、暗号化ソフトウエアを生成するとともにこの暗号化ソフトウエアと２以上の基本アルゴリズムの組合せ情報を前記ソフトウエア復号化処理に引き渡す処理を含み、

前記ソフトウア復号化処理は、前記基本アルゴリズムの組合せ情報に基づいて自身の保有する復号化アルゴリズムを選択して前記暗号化ソフトウエアを復号化する処理を含むソフトウエア暗号化・復号化方法。

【請求項２】　前記ソフトウエア復号化ステップは、前記基本アルゴリズムの組合せ情報と前記アルゴリズムに対する鍵情報とで前記暗号化ソフトウエアの復号化する処理を含む請求項１記載のソフトウエア暗号化・復号化方法。

【請求項３】　ソフトウエアを提供するソフトウエア提供手段と、

２以上の基本アルゴリズムを提供するアルゴリズム提供手段と、

前記アルゴリズム提供手段に提供された基本アルゴリズムの中から少なくとも２以上の基本アルゴリズムを選択する選択手段と、

前記ソフトウエア提供手段から読み出したソフトウエアを、選択手段によって選択結合された２以上の基本アルゴリズムで暗号化する暗号化実行手段と、

暗号化実行手段から出力された暗号化ソフトウエアを出力する出力手段とからなるソフトウエア暗号化システム。

【請求項４】　請求項３のソフトウエア暗号化システムは、前記選択手段により選択された２以上の基本アルゴリズムの結合順序を記録する結合順序記録手段を有しており、

前記出力手段は、暗号化ソフトウエアとともに前記結合順序記録手段から得られた結合順序データを出力する請求項３記載のソフトウエア暗号化システム。

【請求項５】　前記暗号化実行手段は、読み出したソフトウエアを特定のビット数毎の所定数のビット群に分割して前記ビット群のそれぞれに対して並行に前記選択手段で選択結合された２以上の基本アルゴリズムで暗号化処理を行い、暗号化された前記ビット群を結合する請求項３記載のソフトウエア暗号化装置。

【請求項６】　前記暗号化実行手段は、読み出したソフトウエアを特定のビット数毎の所定数のビット群に分解して前記ビット群のそれぞれに対して順番に前記選択手段で選択結合された２以上の基本アルゴリズムで暗号化処理を行い、暗号化された前記ビット群を結合する請求項３記載のソフトウエア暗号化装置。

2

【請求項７】　暗号化されたソフトウエアを提供する暗号化ソフトウエア提供手段と、

２以上の基本アルゴリズムを提供するアルゴリズム提供手段と、

前記アルゴリズム提供手段に提供された基本アルゴリズムの中からソフトウエアの復号に必要な特定の２以上の基本アルゴリズムを選択する選択手段と、

前記選択手段により選択された２以上の基本アルゴリズムの結合順序を記録する結合順序記録手段と、

前記暗号化ソフトウエア提供手段から提供された暗号化ソフトウエアを、選択手段によって選択結合された２以上の基本アルゴリズムで復号化する復号化実行手段とからなるソフトウエア復号化システム。

【請求項８】　前記アルゴリズム提供手段は、２以上の基本アルゴリズムを実行プログラム化して外部から物理的に保護された記録媒体内に保持されたものである請求項７記載のソフトウエア復号システム。

【請求項９】　前記アルゴリズムの組合せ情報は更新可能であり、このアルゴリズムの組合せ情報は旧版の２以上の基本アルゴリズムの組み合わせによって暗号化されて更新組合せ情報として前記ソフトウエア復号化処理に引き渡されることを特徴とする請求項１記載のソフトウエア暗号化・復号化方法。

【発明の詳細な説明】

【０００１】

【発明が属する技術分野】本発明は、文字、音声、動画像、静止画またはプログラム等のデータを暗号化する技術、および暗号化されたこれらのデータを復号化する技術に関する。

【０００２】

【従来の技術】ソフトウエアの流通形態として、文字、音声、動画像、静止画またはプログラム等のデータを暗号化してフロッピーディスク、ＣＤ－ＲＯＭやＭＯ等の媒体に格納して販売する方式や、前記データを暗号化して通信回線を通じてユーザーに配信する方式等が採用されている。

【０００３】このような従来の暗号化方式では、提供者（プロバイダー）はたとえばプログラムを単一のアルゴリズムで暗号化してユーザーに提供し、ユーザーはこれを前記プロバイダーから提供された「鍵」と呼ばれる暗号処理ソフトウエアで復号する作業を行っている。

【０００４】しかしながら、ユーザー側にある暗号処理ソフトウエアは不正ユーザーにより解読されると、この解読結果に基づくコピーツールが作成されてしまう恐れがあり、このようなコピーツールが大量に出回ることによりプロバイダーは大きな損失を被ることにもなりかねない。

3

【０００５】
【課題を解決するための手段】本発明は、このような問題に鑑みてなされたものであり、この種のソフトウエアが短期的にバージョンアップされる特性に着目して、暗号化のアルゴリズムをバージョンアップ毎または定期的に変更可能な暗号化組合せ方式を提供することにある。
【０００６】本発明は、ソフトウエアを暗号化する際に、２以上の暗号化基本アルゴリズムを採用するようにした。ここで暗号化基本アルゴリズムとは、入力データ列を攪乱するために必要な最低限の処理をいう。この処理はたとえば入力データ列を組み替えること、置き換えること、または他の乱数列との排他的論理和をとること等を意味している。
【０００７】一方、ソフトウエア復号化処理（ソフトウエア暗号化装置）ではこの２以上の暗号化基本アルゴリズムに対応した復号アルゴリズムを用意した。そして、ソフトウエア暗号化装置は暗号化ソフトウエアとともに暗号化したアルゴリズムの組合せ情報をソフトウエア復号手段（ソフトウエア復号化装置）に引き渡す。
【０００８】ソフトウエア復号手段は、前記基本アルゴリズムの組合せ情報に基づいて自身の保有する復号アルゴリズムを選択して前記暗号化ソフトウエアを復号化するようにした。
【０００９】前記した手段において、ソフトウエアは暗号化装置に入力されると、任意のアルゴリズムの組合せ（たとえばＡ１およびＡ３）によって暗号化される。このように暗号化されたソフトウエアは、ＣＤ－ＲＯＭあるいは通信回線を通じて流通されてユーザーに届く。ユーザーは自身が保有する復号装置においてこの暗号化ソフトウエアを復号化するが、このときユーザーは暗号化装置で用いた暗号の組合せ情報（たとえばＡ１｜｜Ａ３）に基づいて当該暗号化ソフトウエアを復号する。この組合せ情報は暗号化ソフトウエアとともに同一媒体でユーザーのもとに到着するようにしてもよいし、あるいは別媒体または図示しない鍵情報「Ｋ」とともにユーザーに伝えられるようにしてもよい。また、この組合せ情報は、更新前のアルゴリズムを用いて暗号化してもよい。
【００１０】このようにすれば、たとえば個々では解析容易な程度の低い基本アルゴリズムであっても組み合わせて暗号化することにより解析の困難性を高めることができる。このことは、たとえば個々の基本アルゴリズムは容易に把握可能なものであっても、この基本アルゴリズムの組合せは膨大な数にのぼるため、この組合せそのものを解析するのには多大な労力と時間が必要となり、事実上解析が困難になる。また、仮に解析が可能になったとしても、ソフトウエアのバージョンアップによってさらにアルゴリズムの新しい組合せでソフトウエアが暗号化されるため、最近の短期なサイクルでのソウトウエアのバージョンアップに十分に対応できる。

4

【００１１】したがって、この暗号化ソフトに挑戦するためにハッカーは無数の組合せの暗号アルゴリズムに直面しなくてはならず、事実上解読作業を断念せざるを得なくなる。
【００１２】
【発明の実施の形態】以下、図面に基づいて、本発明の実施の形態を説明する。図１に示すように、本発明では、ソフトウエアを暗号化する際に、２以上の暗号化基本アルゴリズムを採用するようにした。一方、ソフトウエア復号化処理（ソフトウエア暗号化装置）ではこの２以上の暗号化基本アルゴリズムに対応した復号アルゴリズムを用意した。そして、ソフトウエア暗号化装置は暗号化ソフトウエアとともに暗号化した基本アルゴリズムの組合せ情報をソフトウエア復号手段（ソフトウエア復号化装置）に引き渡す。
【００１３】ソフトウエア復号手段は、前記基本アルゴリズムの組合せ情報に基づいて自身の保有する復号アルゴリズムを選択して前記暗号化ソフトウエアを復号化するようにした。
【００１４】これにより、ソフトウエアは暗号化装置に入力されると、任意の基本アルゴリズムの組合せ（たとえばＡ１およびＡ３）によって暗号化される。このように暗号化されたソフトウエアは、ＣＤ－ＲＯＭあるいは通信回線を通じて流通されてユーザーに届く。ユーザーは自身が保有する復号化装置においてこの暗号化ソフトウエアを復号化するが、このときユーザーは暗号化装置で用いた暗号の組合せ情報（たとえばＡ１｜｜Ａ３）に基づいて当該暗号化ソフトウエアを復号する。この組合せ情報は暗号化ソフトウエアとともに同一媒体でユーザーの元に到着するようにしてもよいし、あるいは別媒体または図示しない鍵情報「Ｋ」とともにユーザーに伝えられるようにしてもよい。
【００１５】図２および図１３は、本発明の実施例であるソフトウエア暗号化装置のハードウエア構成を示している。コンピュータ本体（ＢＤＹ）にはＩＣカードスロット（ＩＣＲ）とフロッピーディスクドライブ（ＦＤ）が設けられている。また図には示していないがコンピュータ本体（ＢＤＹ）にはモデム（ＭＤＭ）や受信装置が内蔵されており、有線または無線経路を通じて外部とデータの送受信が可能である。
【００１６】コンピュータ本体（ＢＤＹ）には入力装置としてキーボード（ＫＥＹ）およびマウス（ＭＯＵ）が接続されている。またコンピュータ本体（ＢＤＹ）には出力装置としてディスプレイ（ＣＲＴ）およびプリンタ（ＰＲＮ）が接続されている。
【００１７】コンピュータ本体（ＢＤＹ）にはさらに外部記憶装置として光ディスクドライブ装置（ＭＯＤ）が接続されている。またコンピュータ本体（ＢＤＹ）内にはハードディスク装置が内蔵されている。
【００１８】図２において、ＢＵＳはバスであり、制御

5

バスおよびデータバスを意味している。ＣＰＵは中央制御部であり、３２ビットまたは６４ビット処理のプロセッサが用いられている。ＭＥＭはメモリであり、後述の暗号組合せテーブルや作業領域が特定のアドレスによって設定される。

【００１９】ソフトウエア提供手段としてはフロッピーディスクのみを図示しているが、これに限らず、光磁気ディスクあるいは通信回線であってもよい。さらに、メモリＭＥＭあるいは中央制御部ＣＰＵ内のバッファもソフトウエア提供手段として機能する。

【００２０】ＩＣＲはＩＣカードリーダであり、ＪＥＩＤＡ準拠のＰＣＭＣＩＡカードを装着することが可能である。本実施例において後述のアルゴリズムプログラムＡ１，Ａ２，Ａ３・・・・Ａｎはこのカードに格納されて提供される。このＩＣカードには物理的なプロテクトを施すことが好ましく、たとえば、ユーザーの不正な開封によってアルゴリズムのデータを消滅させたり、読み出しを禁止するようにしてもよい。さらにこのＩＣカードは所定の期間毎にその複数のアルゴリズムの構成を変更してもよい。一定期間毎にＩＣカード内に格納されるアルゴリズムの配置または内容を更新できるようすれば、ソフトウエアの復号を期間的に限定させることができ、デモソフトあるいは使用に応じた従量制ソフトウエアに対応することができる。

【００２１】ＭＯＤは光磁気ディスク装置であり、１００メガバイト以上の容量を有する光磁気ディスク媒体の読み書きが可能となっている。また、ＩＦは通信インターフェースであり、外部の通信回線と接続されている。

【００２２】なお、以上の装置構成の他に、たとえばＣＤ－ＲＯＭスタンピング装置を接続してもよい。以上図２はソフトウエア暗号化装置として説明したが、これに対応したソフトウエア復号化装置も同様の構成を有している。ただし、当該装置をソフトウエア復号化装置として用いる場合には、ＣＤ－ＲＯＭドライブを設けてもよい。すなわち、音声、静止画、動画像等の大量データを流通させる媒体としてはＣＤ－ＲＯＭが適しているためである。

【００２３】図３は、本実施例のシステム構成を機能ブロックで表したものである。同図において上段はソフトウエア暗号化装置の機能を示しており、下段はソフトウエア復号化装置の機能を示している。

【００２４】図３の機能と図２で説明したハードウエアとの関係を説明すると、図３におけるアルゴリズムプログラム（Ａ１，Ａ２・・・・Ａｎ）はＩＣカードに格納されて提供されている。また選択処理、結合処理、結合プログラム処理は中央制御部（ＣＰＵ）によって実現される機能である。鍵情報「Ｋ」はキーボード（ＫＥＹ）より入力される。また、ソフトウエア格納ファイルはフロッピーディスク装置（ＦＤ）または光磁気ディスク装置（ＭＯＤ）を通じて入力されてメモリ（ＭＥＭ）上に

6

読み込まれる。

【００２５】次に、図３を用いてソフトウエアの暗号化処理について説明する。まず、中央制御部（ＣＰＵ）の選択処理によりソフトウエアの暗号化処理に用いられるアルゴリズムを決定する。ここでは２以上の基本アルゴリズムプログラムを決定する処理が行われる。基本アルゴリズムの決定は、たとえばメモリ（ＭＥＭ）上に設定される図４に示すようなアルゴリズムテーブルを用いてもよい。

【００２６】アルゴリズムテーブルには同図に示すように、Ａ１，Ａ２・・・Ａｎのｎ個の基本アルゴリズムが行列状に設定されている。このようにｎ個の基本要素（アルゴリズム）から重複を許可して２個の結合アルゴリズムを用いる場合ｎの２乗の結合アルゴリズムを生成できる。

【００２７】一方、ｎ個の基本要素（アルゴリズム）から任意の個数をタンデム接続してその組合せを考えた場合、各要素（アルゴリズム）の並び替えを行った場合、最大ｎ！個の結合アルゴリズムを得ることができる。さらに、重複並び替えを許可した場合、最大ｎのｎ乗の個数の結合アルゴリズムを生成できる。

【００２８】たとえばアルゴリズムＡ１とＡ２とを組み合わせてＡ１｜｜Ａ２とすることもできるし、３個のアルゴリズムの組合せによってたとえばＡ１｜｜Ａ２｜｜Ａ３とすることもできる。また同一のアルゴリズムをＬ段組み合わせてたとえばＡ１｜｜Ａ１｜｜Ａ１｜｜・・・・｜｜Ａ１としてもよい。

【００２９】このように本実施例では基本アルゴリズムの組合せが多数生成できるため、たとえば個々の基本アルゴリズムとしては解析容易であっても組合せ結合によって解析困難なアルゴリズムとして用いることができる。

【００３０】次に、具体的なアルゴリズムの例について説明する。図５は、転置型基本アルゴリズムの具体例を示している。すなわち、本アルゴリズムでは鍵連動交換スイッチがプログラムとして設定されており、８ビットのデータ毎にビット位置が入れ替えられて出力されるようになっている。入れ替え位置を制御するのが外部から与えられる鍵情報「Ｋ」である。なお同図では入出力を８ビット構成としているが、これに限定されない。このような転置型基本アルゴリズムはたとえば前述のアルゴリズムテーブルに「Ａ１」として登録されている。

【００３１】図６は、換字型基本アルゴリズムの具体例を示している。このアルゴリズムでは入力データに対して出力するデータをテーブル化して保有している。なお同図では入出力を３ビット構成としているがこれに限られないことはいうまでもない。このような換字型基本アルゴリズムはたとえば前述のアルゴリズムテーブルに「Ａ２」として登録されている。

【００３２】図７は、排他アルゴリズムの具体例を示し

ている。本アルゴリズムでは、たとえば入力された各ビットに対して鍵情報「K」を用いて排他論理処理を行う。なお同図では入出力を３ビット構成としているがこれに限られないことはいうまでもない。このような排他アルゴリズムはたとえば前述のアルゴリズムテーブルに「Ａ３」として登録されている。

【００３３】図８は、乗算型基本アルゴリズムの具体例を示している。この図では８ビットのデータが入力されると、鍵情報「K」によって乗算器で当該入力データが乗算された後、出力マスキング回路によってマスクされたデータが出力される。このような乗算型アルゴリズムはたとえば前述のアルゴリズムテーブルに「Ａ４」として登録されている。

【００３４】以上のような複数のアルゴリズムからアルゴリズムが中央制御部（ＣＰＵ）の「選択処理」により選択されると、結合処理（暗号化実行手段）が行われる。この結合処理の具体例を示したものが図９および図１０である。

【００３５】図９はＤＥＳ型結合の一例を示したものである。同図において、ソフトウエアデータが入力されると、これを所定のビット毎（たとえば８ビット毎）に分割して処理を行う。ここでは、前記８ビット中の上位４ビットを左半分データ（Ｄ１）、下位４ビットを右半分データ（Ｄ２）に分割する。

【００３６】そして、右半分データ（Ｄ２）はＡ１アルゴリズムによって処理され暗号化データＣ１として出力される。左半分データ（Ｄ１）は、前記暗号化データ（Ｃ１）と排他論理処理されて暗号化データ（Ｄ１＋Ｃ１）として出力される。

【００３７】一方、左半分データ（Ｄ１）とＡ１アルゴリズムの出力データ（Ｃ１）の排他論理処理出力データは、Ａ２アルゴリズムで処理されて暗号化データＣ２として出力される。この暗号化データＣ２は、右半分データ（Ｄ２）と排他論理処理されて、暗号化データ（Ｄ２＋Ｃ２）として出力される。

【００３８】なお、図９の復号処理については図は省略するが、図９の「Ａ１プログラム」（Ａ１の復号アルゴリズム）と「Ａ２プログラム」（Ａ２の復号アルゴリズム）を入れ替えたシステムを用意すればよい。

【００３９】図１０は、ＥＮＩＧＭＡ結合の一例を示したものである。この例では入力されたソフトウエアをＡ１アルゴリズムで一次変換した後、Ａ２プログラムで二次変換する

また同図左半部に示しているように、これを復号化する場合には、まずアルゴリズムＡ２の復号アルゴリズム$A2^{-1}$にて一次復号を行った後、アルゴリズムＡ１の復号アルゴリズム$A1^{-1}$にて二次復号を行うことによって元のソフトウエアに戻すことができる。

【００４０】次に図１１を用いて、アルゴリズムとして転置型アルゴリズム（Ａ１）と換字型アルゴリズム（Ａ２）を結合してＥＮＩＧＭＡ型結合処理を行う場合についてさらに具体的な実例によって説明する。

【００４１】まず、鍵連動交換スイッチに対して鍵情報「K」が与えられる。この鍵情報「K」は入力される８ビットデータに対して出力をどのビットに転置するかを規定した情報である。同図では第１ビット→第７ビット、第２ビット→第３ビット、第３ビット→第２ビット、第４ビット→第５ビット、第５ビット→第１ビット、第６ビット→第８ビット、第７ビット→第６ビット、第８ビット→第４ビットに設定された鍵情報「K」が鍵連動交換スイッチに与えられている。

【００４２】ここで、ソフトウエアデータ（平文データ）として「０Ｆｈ」、すなわち「００００１１１１」が与えられると、前述の鍵情報「K」により規定された鍵連動交換スイッチにより第１ビットの「０」は第７ビットへ、第２ビットの「０」は第３ビットへ、第３ビットの「０」は第２ビットへ、第４ビットの「０」は第５ビットへ、第５ビットの「１」は第１ビットへ、第６ビットの「１」は第８ビットへ、第７ビットの「１」は第６ビットへ、第８ビットの「１」は第４ビットへそれぞれ転置される。この結果、アルゴリズムＡ１による変換結果は「１００１０１０１」すなわち「９５ｈ」となる。

【００４３】次にアルゴリズムＡ１によって一次暗号化されたデータ「９５ｈ」を換字型アルゴリズムＡ２によって二次暗号化する。ここではまず、入力データ（９５ｈ）を上位４ビットの左半分データと、下位４ビットの右半分データとに分割してそれぞれの変換テーブルに基づいて変換を行う。この結果、二次暗号化出力データは「００１００００」すなわち「２０ｈ」となる。

【００４４】次に、図３に示すように、以上の選択処理、結合処理および結合プログラム処理が行われて暗号ソフトエウアが生成されると、この暗号化ソフトウエアはMO、ＣＤ－ＲＯＭ、フロッピーディスク等の媒体に格納されて提供者よりユーザーに配送される。また、インターフェース（Ｉ／Ｏ）を通じて通信回線を経由してユーザーのもとに配信されるようにしてもよい。またこのとき、アルゴリズムの選択順番コード、たとえば前述の例では「Ａ１｜｜Ａ２」というコードがMO、ＣＤ－ＲＯＭ、フロッピーディスク等の媒体に暗号化ソフトウエアとともに格納される。また通信による場合は暗号化ソフトウエアとともに通信路に送出される。

【００４５】なお、この選択順番コードは前記暗号化ソフトウエアとは別の配信経路、たとえば電話による口頭説明等で提供者よりユーザーに伝えられてもよい。さらに鍵情報「K」とともに選択順番コードをユーザーに提供してもよい。

【００４６】前記暗号化ソフトウエアと選択順番コードを受信したユーザー側の復号化装置では、前記選択順番コードの情報に基づいて復号アルゴリズムを選択して結

9

合処理および結合プログラム処理を行って復号化ソフトウエアを得る。

【００４７】この復号処理の具体例を示したものが図１２である。同図において、暗号化ソフトウエアより暗号化データが８ビットずつ（２０ｈ）入力されると、その上位４ビットと下位４ビットとをそれぞれ左半分データ、右半分データとしてアルゴリズムＡ２$^{-1}$による換字変換がまず実行される。この換字変換により得られた一次復号化データ（９５ｈ）は、さらに転置型アルゴリズムＡ１$^{-1}$による転置変換が行われ復号データとして「００００１１１１」すなわち「０Ｆｈ」が得られる。

【００４８】ところで、アルゴリズムの組合せ情報（図１１の例ではＡ１｜｜Ａ２）と鍵情報「Ｋ」とが一旦外部に漏洩されてしまうと暗号化ソフトウエアの解読は極めて容易になってしまう。そこで、たとえば組合せ情報と鍵情報に対してさらに２以上の基本アルゴリズムを組み合わせて暗号化し、これを復号化情報として提供者からユーザーに伝える。

【００４９】これを受け取ったユーザーは初期鍵によってこの暗号化された復号化情報を復号して前記暗号化ソフトウエアの復号に必要な組合せ情報と鍵情報とを得る。前記復号化情報は定期的に更新され、新たな復号化情報は、旧版の復号化情報中の組合せ情報を用いて生成される。

【００５０】したがって、ユーザーは復号化情報を復号するためには常に一世代前の直近の復号化情報中の組合せ情報が必要になる。これにより、いずれかの時点での暗号化キー情報が外部に漏洩したとしても、一世代前の直近の暗号化キー情報を有していなければ暗号化ソフトウエアを解読（復号）することは困難になる。

【００５１】

【発明の効果】本発明によれば、個々では解析容易な程度の低い基本アルゴリズムであっても組み合わせて暗号化することにより解析の困難性を高めることができる。このことは、たとえば個々の基本アルゴリズムは容易に把握可能なものであっても、この基本アルゴリズムの組

10

合せは膨大な数にのぼるため、この組合せそのものを解析するのには多大な労力と時間が必要となり、事実上解析が困難になる。また、仮に解析が可能になったとしても、ソフトウエアのバージョンアップによってさらにアルゴリズムの新しい組合せでソフトウエアが暗号化されるため、最近の短期なサイクルでのソウトウエアのバージョンアップに十分に対応できる。

【図面の簡単な説明】

【図１】　本発明の原理図

【図２】　実施の形態のハードウエアの構成図

【図３】　実施の形態のシステム構成の機能ブロック図

【図４】　実施の形態のアルゴリズムテーブルを示す説明図

【図５】　転置型アルゴリズムの具体例を示す説明図

【図６】　換字型アルゴリズムの具体例を示す説明図

【図７】　排他アルゴリズムの具体例を示す説明図

【図８】　乗算型アルゴリズムの具体例を示す説明図

【図９】　ＤＥＳ型結合処理の具体例を示す説明図

【図１０】　ＥＮＩＧＭＡ結合の具体例を示す説明図

【図１１】　転置型アルゴリズム（Ａ１）と換字型アルゴリズム（Ａ２）を結合してＥＮＩＧＭＡ型結合処理を行う場合の具体例を示す説明図

【図１２】　図１１の結合処理で暗号化された暗号化ソフトウエアを復号化する場合の具体例を示す説明図

【図１３】　実施の形態のハードウエア構成を示す説明図

【符号の説明】

ＣＰＵ・・中央制御部

ＫＥＹ・・キーボード

ＦＤ・・フロッピーディスク装置

ＩＣＲ・・ＩＣカードリーダ

ＭＥＭ・・メモリ

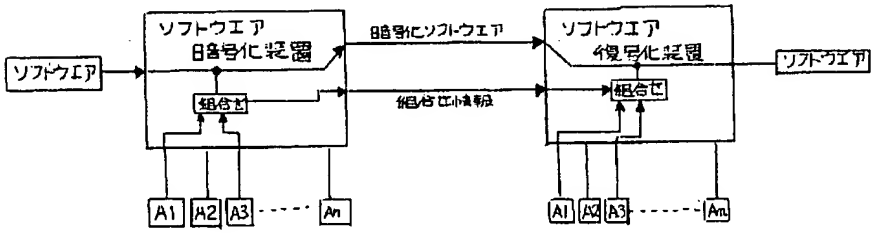
ＭＯＤ・・光磁気ディスク装置

ＭＯ・・光磁気ディスク

Ｉ／Ｆ・・通信インターフェース

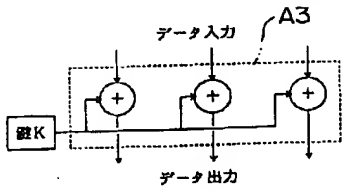
【図１】

本発明の原理図



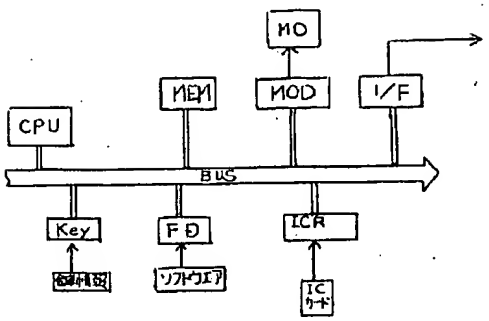
【図７】

排他アルゴリズムの具体例を示す説明図



【図２】

実施例のハードウエアの構成図



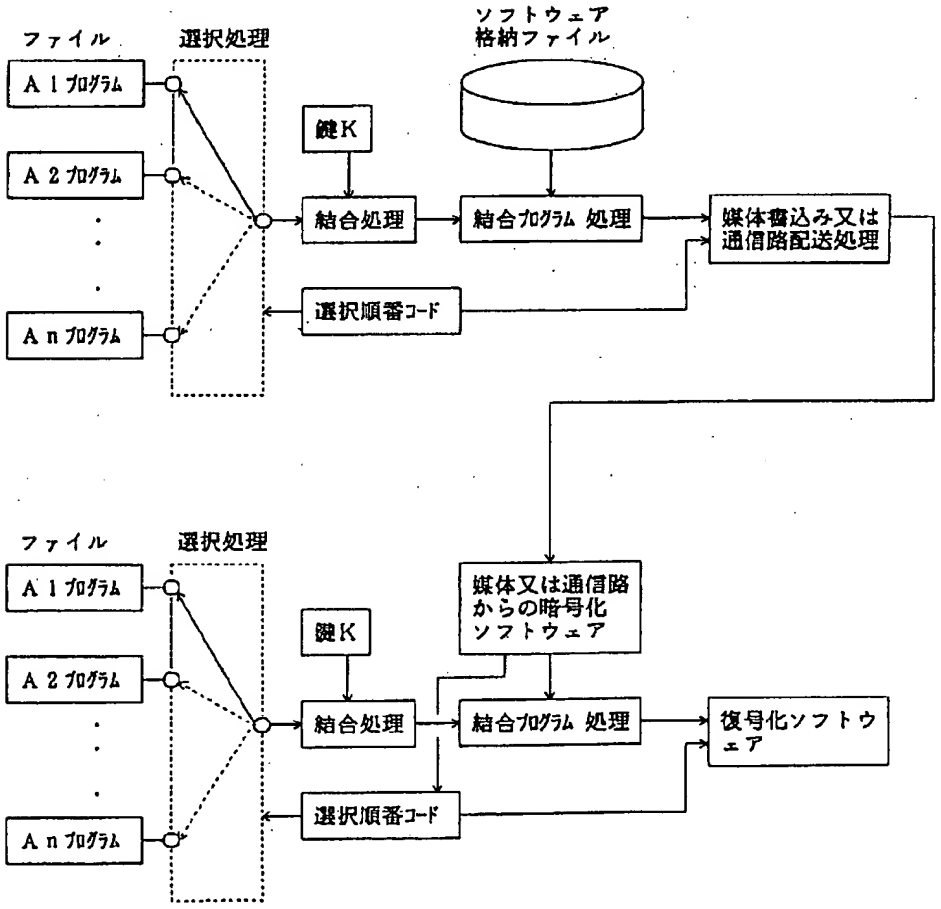
【図４】

実施例のアルゴリズムテーブルを示す説明図

		各種アルゴリズム			
	↱	A 1	A 2	・・・　・・・	A n
各種アルゴリズム	A 1	A 11	A 12		A 1n
	A 2	A 21	A 22		A 2n
	・ ・ ・			・　・ 　・ 　　・	
	A n	A n1	A n2		A nn

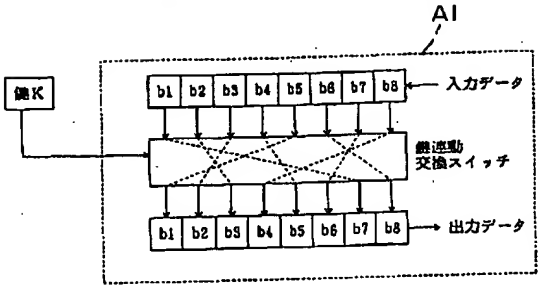
【図３】

実施例のシステム構成の機能ブロック図



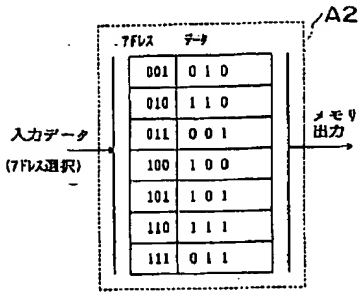
【図５】

転置型アルゴリズムの具体例を示す説明図



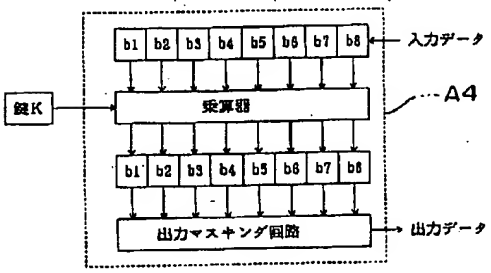
【図６】

換字型アルゴリズムの具体例を示す説明図



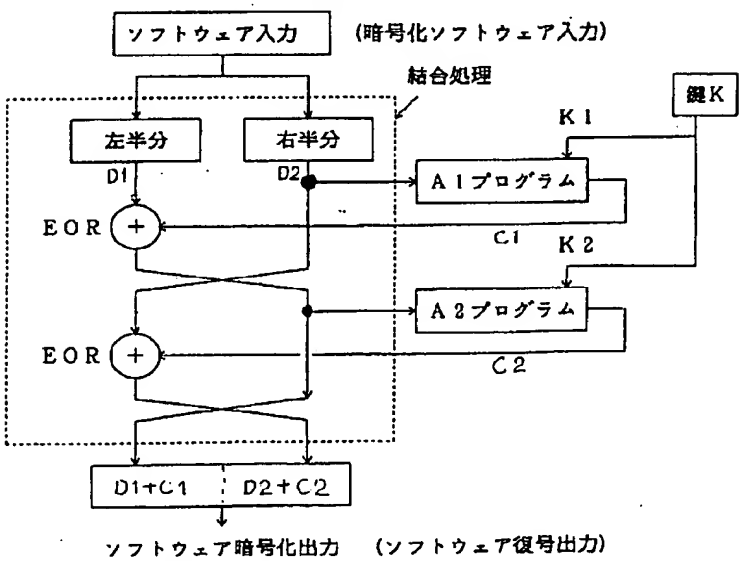
【図８】

乗算型アルゴリズムの具体例を示す説明図



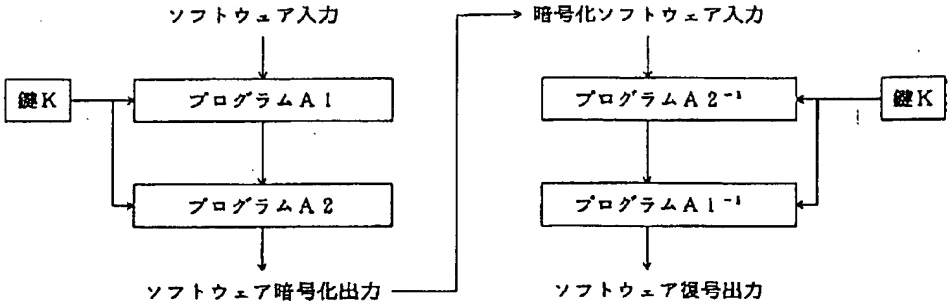
【図９】

ＤＥＳ型結合処理の具体例を示す説明図



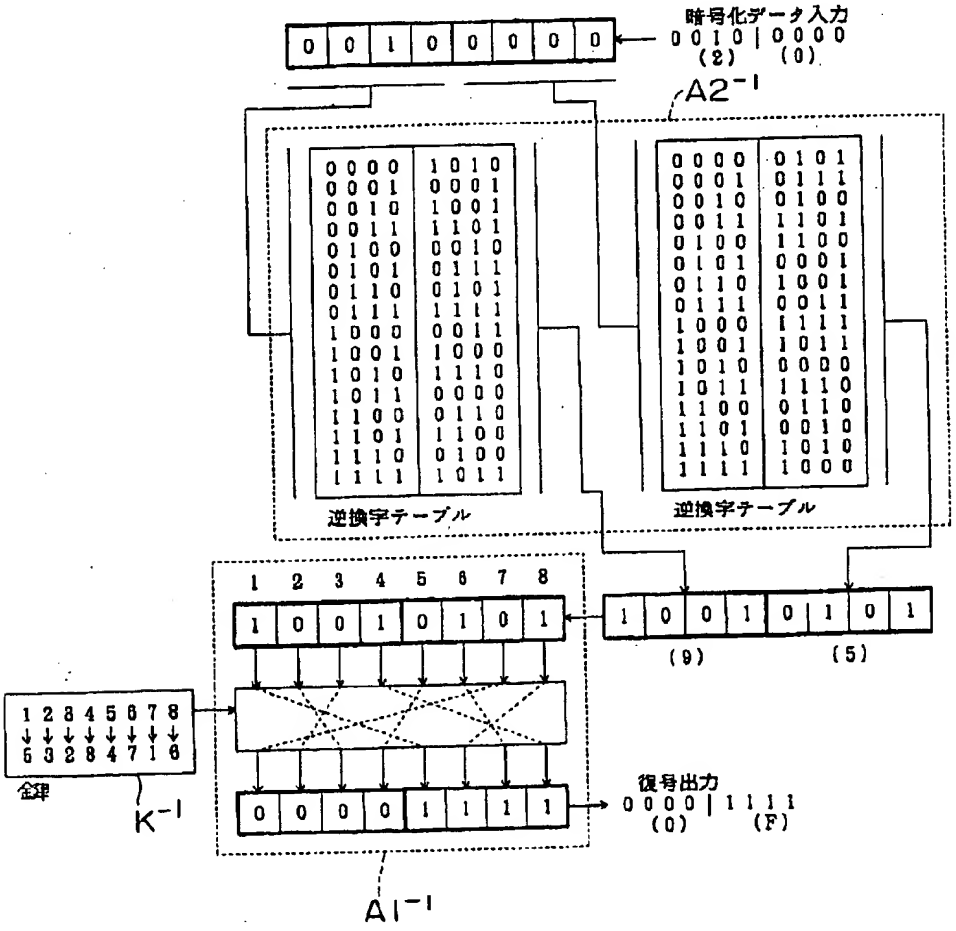
【図１０】

ＥＮＩＧＭＡ結合の具体例を示す説明図



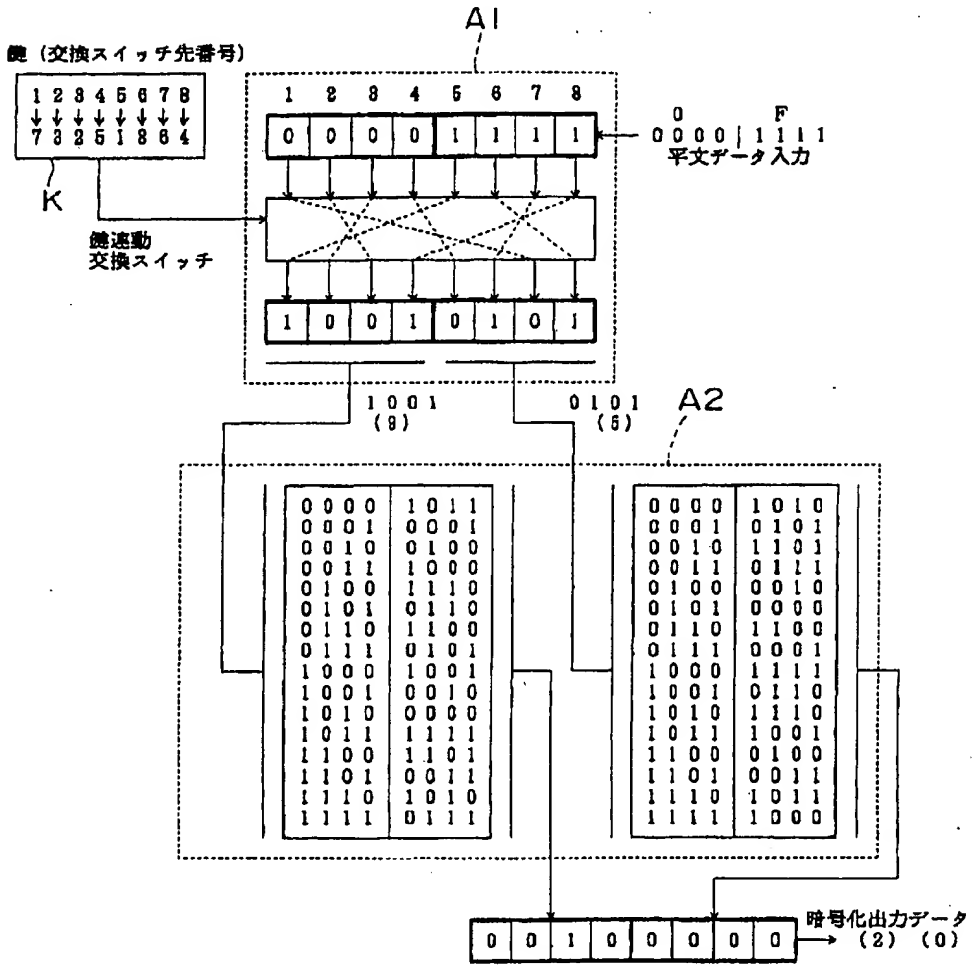
【図１２】

図１１の結合処理で暗号化された暗号化ソフトウエアを復号化する場合の具体例を示す説明図



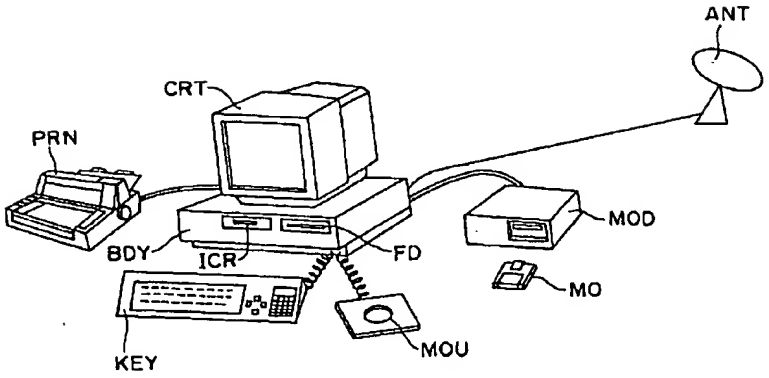
【図１１】

転置型アルゴリズム（Ａ１）と換字型アルゴリズム（Ａ２）を結合してＥＮＩＧＭＡ型結合処理を行う場合の具体例を示す説明図



【図１３】

実施例のハードウエア構成を示す説明図



Japanese Patent Laid-open No. HEI 8-286904 A
Publication date : November 1, 1996
Applicant : Fujitsu Limited

Title : SOFTWARE ENCRYPTION AND DECODING METHOD, SOFTWARE ENCRYPTION SYSTEM, AND SOFTWARE DECODING SYSTEM

[ABSTRACT]

[Problem] To prevent the illegal decryption of encrypted software by simple technique.

[Solving Means] Not less than two encryption basic algorithms are used to encrypt a software. Decoding algorithms corresponding to the not less than two encryption basic algorithms are prepared, respectively, for a software decoding processing. In a software encryption processing, encrypted combination information on encryption basic algorithms as well as an encrypted software are transferred to a software decoding processing. In the software decoding processing, inverse algorithms held by the unit are selected based on the basic algorithm combination information, and the encrypted software is decoded using the selected algorithms.

Best Available Copy

[Claim 1]A software encryption and decoding method comprising:

a software encryption step of encrypting a software using a combination of not less than two encryption basic algorithms; and

a software decoding step of inputting the encrypted software, and decoding the software based on decoding algorithms corresponding to the not less than two encryption basic algorithms used for encryption, wherein

in a software encryption processing, the encrypted software is generated, and

the encrypted software and combination information on the not less than two basic algorithms is transferred to a software decoding processing, and

in the software decoding processing, decoding algorithms held by a software decoding device are selected based on the combination information on the basic algorithms, and the encrypted software is thereby decoded.

[0012]

[MODE FOR CARRYING OUT THE INVENTION]

The embodiment of the present invention will be explained hereinafter with reference to the drawings. As shown in Fig. 1, the present invention adopts not less than two encryption basic algorithms to encrypt a software. Decoding algorithms corresponding to the encryption basic algorithms are prepared for a software decoding processing (software encryption device). The software encryption device transfers combination information on encrypted basic algorithms as well as an encrypted software to the software decoding unit (software decoding device).

[0013] The software decoding unit selects decoding algorithms held by the unit itself based on the basic algorithm combination information, and decodes the encrypted software.

[0014] By doing so, if a software is input to the encryption device, the software is encrypted based on an arbitrary basic algorithm combination (e.g., algorithms A1 and A3). The software thus encrypted arrives at a user through a CD-ROM or a communication line. The user decodes this encrypted software by the decoding device that the user owns. During decoding, the user decodes the encrypted software based on encryption combination information (e.g., A1 | | A3) employed in the encryption device. This combination information may arrive at the user by the same

medium as that for the encrypted software or may be conveyed to the user by a different medium or as key information "K", not shown.